Quantum Computers: Should we worry?

Dr. Morton Swimmer
FTR, Trend Micro Research

HH.Security Meetup 2024-12-5

NATO OTAN NORTH ATLANTIC TREATY ORGANIZATION

ABOUT US | WHAT WE DO | NEWSROOM | WORK WITH US | LEARN MORE

Newsroom > Official texts

Summary of NATO's Quantum Technologies Strategy

16 Jan. 2024 - | Last updated: 17 Jan. 2024 11:32

English | French

- NATO has developed, adopted and implemented frameworks, policies and standards for both software and hardware to enhance interoperability;
- Allies have cooperated in the development of quantum technologies with a view to maintain NATO's technological edge and Allies' abilities in the field;
- NATO has identified, understood and capitalised on evolving quantum technologies advancements, including with enabling technologies and in convergence with other EDTs;
- NATO has a Transatlantic Quantum Community to strategically engage with government, industry and academia from across our innovation ecosystems;
- NATO has transitioned its cryptographic systems to quantum-safe cryptography;
- Relevant quantum strategies, policies and action plans are dynamically updated and executed; and
- Allies have become aware of, and act to prevent, on a voluntary basis, adversarial investments and interference into our quantum ecosystems, which can include, on a national basis, the examination of relevant supply chains.

5. Further, NATO will provide the leading transatlantic forum for quantum technologies

ACCESSWIRE

Why We Can't Afford to Ignore Quantum Computing, Even if We Don't Completely Understand It

TAG Infosphere
Wed, December 4, 2024 at 3:00 PM GMT+1 • 3 min read

Available For Free Download

NEW YORK, NY / ACCESSWIRE /
the fear that the Y2K bug provoked
even panic-that when the calendar
and systems that could only accor
would come crashing down, wreak
many deaths.

If that sounds like a distant memo
about Y2Q, the shorthand cyber ex
Though quantum computing is stil
about it can come across as geeky
danger it poses to the global interr

Experts agree that it's only a matte
technology will be able to crack th
secrets that keep the internet secu
current safeguards with post-quan
potential catastrophe seems years
the quantum technology being dev
advancing.

The new issue of the Security Ann
has four articles and a short story
interview with Peter Shor, the math
quantum algorithm that now bears
will likely be another decade befor
capable of cracking the code. But
to hurry.

QUANTUM COMPUTING KILLS ENCRYPTION

by: Elliot Williams

79 Comments

September 29, 2015

Imagine a world where the most widely-used cryptogra
computers allow encrypted Internet data transactions t
listening. No more HTTPS, no more PGP. It sounds a litt
cryptographers interested in post-quantum crypto are v
threat of quantum computing to cryptography is already
activity in the field, so we felt it was time for a recap.

HOW BAD IS IT?

If you take the development of serious quantum compu
based on factoring primes or doing modular exponentia
and Diffie-Hellman are all in trouble. Specifically, Shor's
will render the previously difficult math problems that u
irrespective of chosen key length. That covers most cur
that's used in negotiating an SSL connection. That is (or
nearly every important encrypted transaction that touch

All is not doom and gloom, however. There are families of public-key algorithms that aren't solved by Shor's algorithm or any of the other known quantum algorithms, although they haven't been subjected to as much (classical) cryptanalysis and the algorithms and protocols aren't as polished yet. (More on this topic below.)

COULD ADVANCED QUANTUM COMPUTING POSE A RISK TO BITCOIN SECURITY?

Rapid progress in quantum computing could pose a risk to certain types of bitcoin transactions. So how can we combat this risk?

DEBANJAN CHATTERJEE • OCT 16, 2021

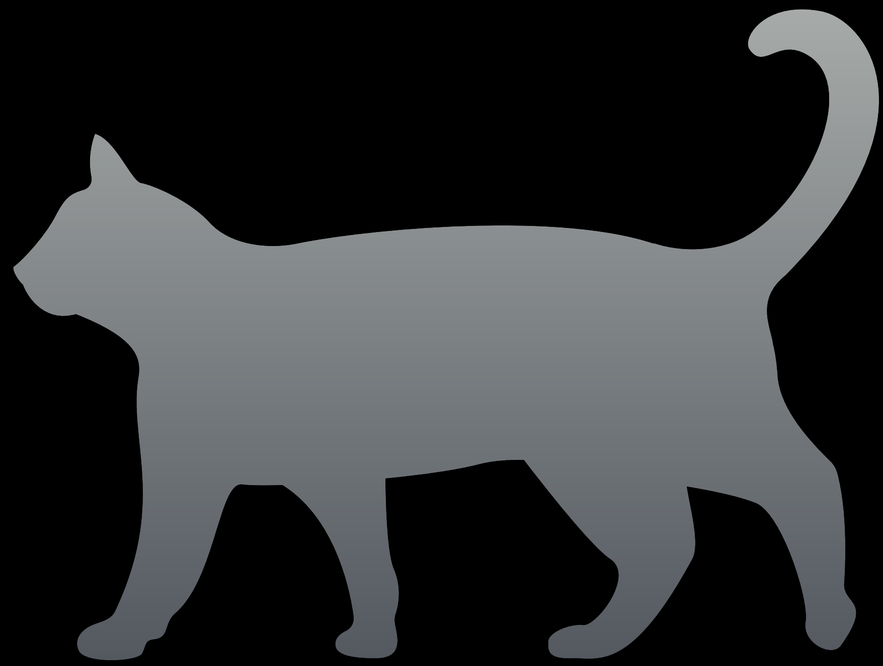
HOME > TECHNICAL

Rapid progress in quantum computing is predicted by some to have crucial ramifications in domains using public-key cryptography, such as the Bitcoin ecosystem.

Bitcoin's "asymmetric cryptography" is based on the principle of "one-way function," implying that a public key can be easily derived from its corresponding private key but not vice versa. This is because classical algorithms require an astronomical amount of time to perform such computations and consequently are impractical. However, Peter Shor's polynomial-time quantum algorithm run on a sufficiently-advanced quantum

Three questions

- What is the threat?
- How real is the threat?
- What can we do about it?




What is the threat?

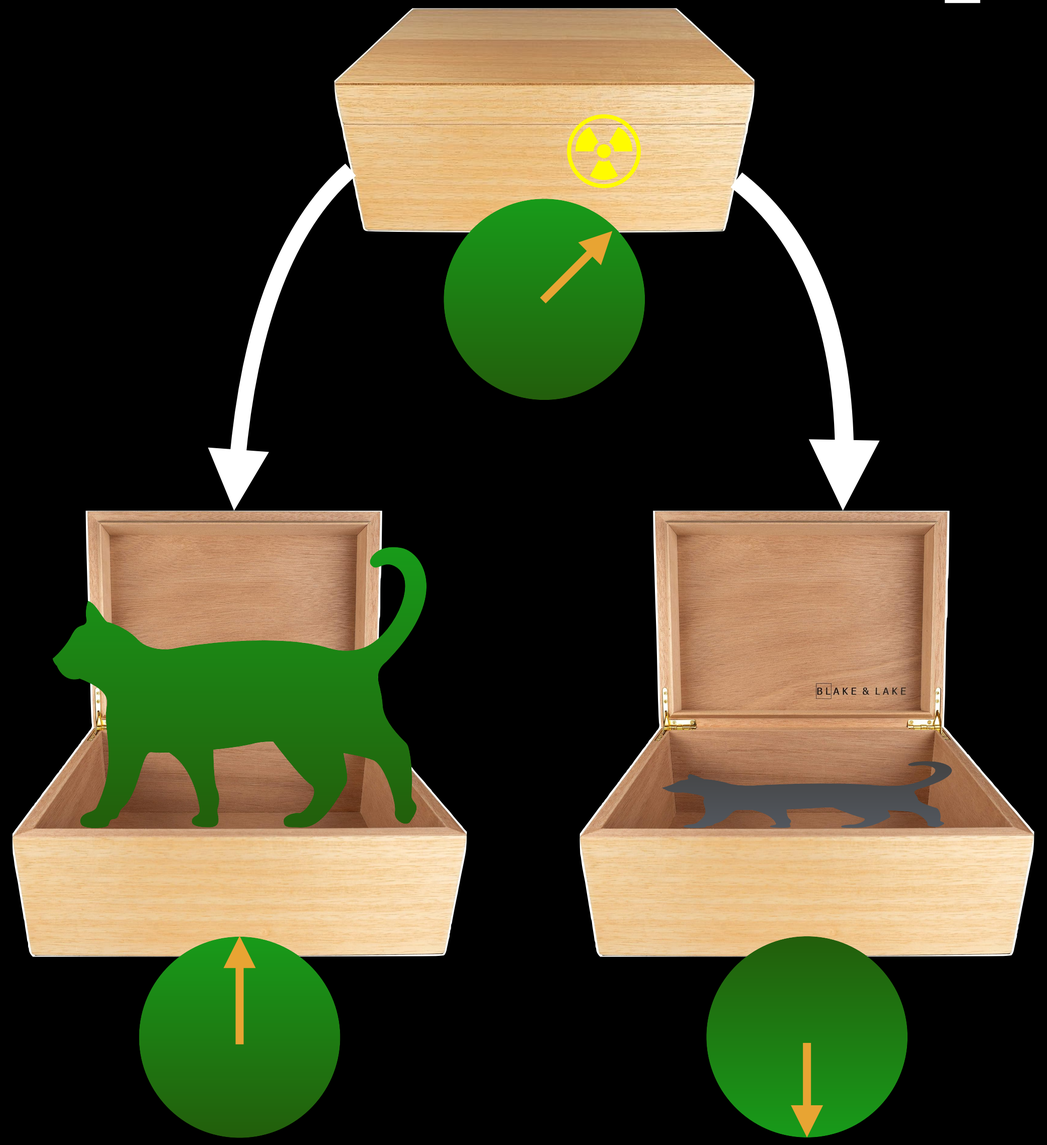
Harvesting attack

- We assume that our communications are secure when encrypted
  - Quantum computers may break this assumption
- Harvesting attack
  - Capture traffic now, decrypt later
  - Requirements on secrecy vary
  - 'later' may be later than we care about or never late enough

Quantum Computers

- Not an evolution of classical
- Based on Superposition and Entanglement
- Built with Qubits and Gates

Superposition



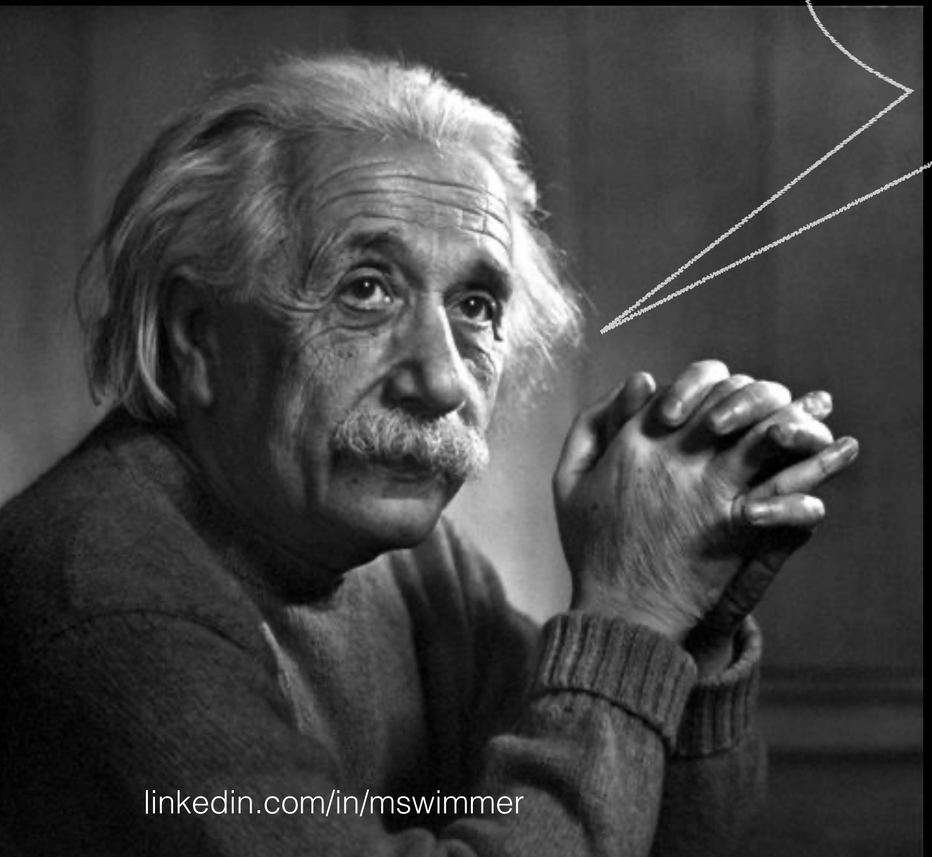
- Classical bit {0,1}
- A qubit {0..1}
- This will "collapse" when measured

Our goal is to create a system that cancels out wrong answers and leaves the right answers

Entanglement

"Verschränkung"

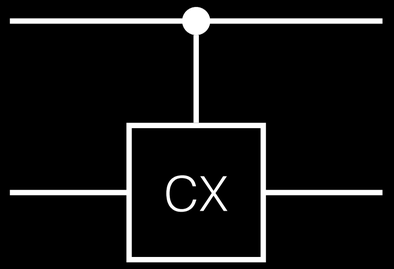
"Spukhafte Fernwirkung"



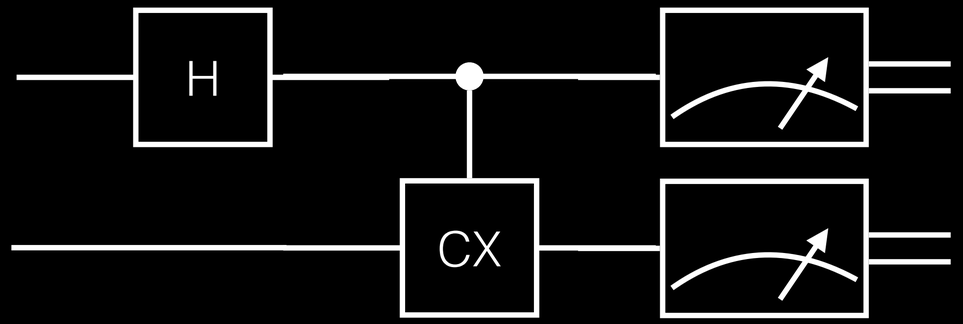
Quantum gates

Hadamard

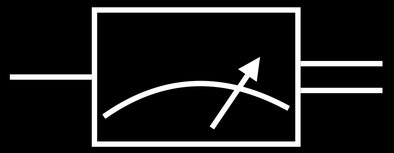
NOT



Controlled NOT



and many more



Measurement

resulting in a classical bit

Breaking RSA

Disclaimer

No cryptographers were permanently damaged in the production of the following slides

BUT, there will be math

Breaking RSA

This means factoring large integers

$$s \times t = N$$

N is shared, s and t are secret

The attacker's goal: find s or t

Factoring is hard: Naive approach

```
def calculate_primes_up_to(n):
    primes = set()
    for a in range(2, int(n/2)+1):
        if not any(a % b == 0 for b in primes):
            primes.add(a)
    return sorted(primes)
```

```
def naive_factor(N, primes):
    for i in primes:
        for j in [p for p in primes if p < i]:
            if i * j == N:
                return i, j
```

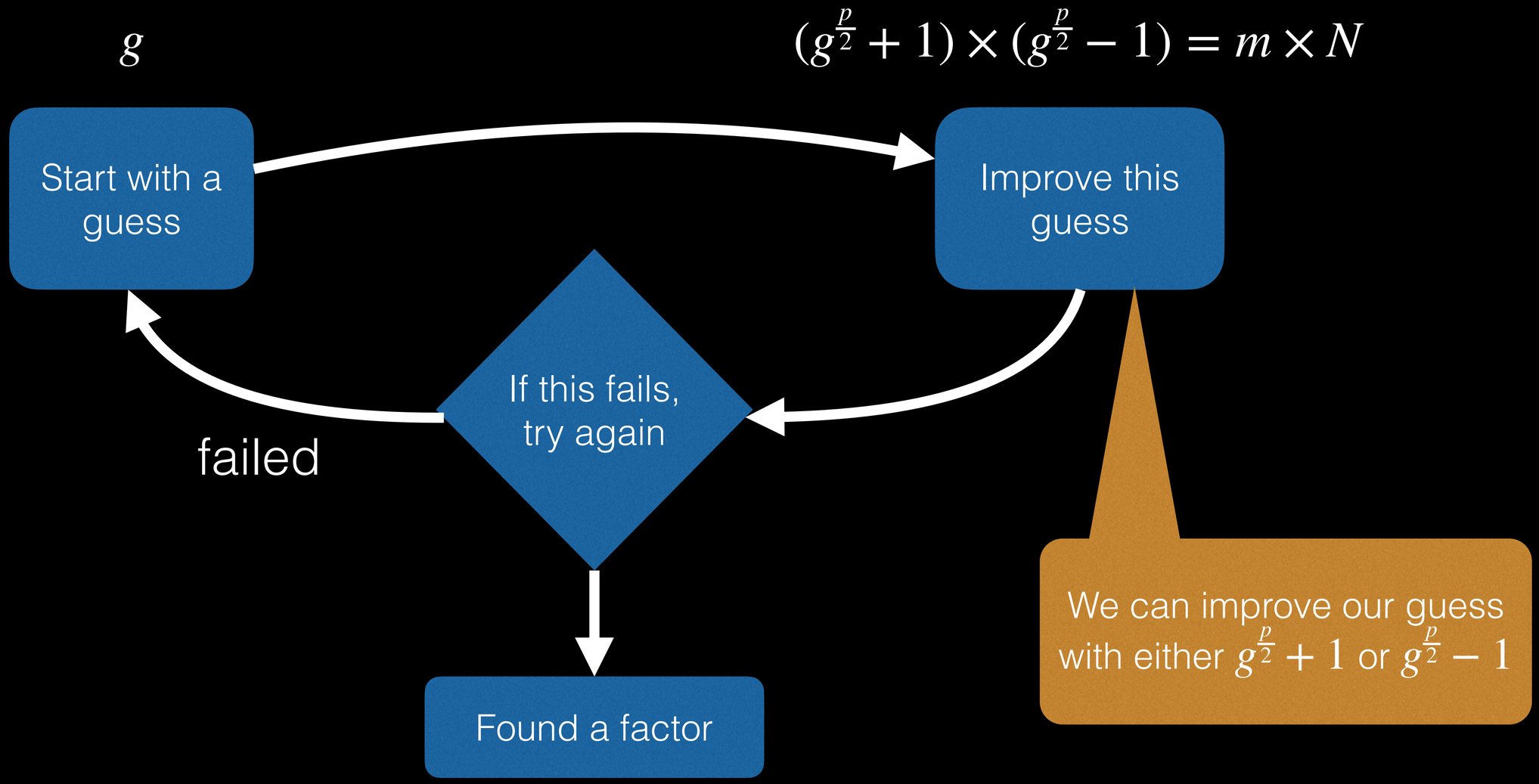
Factor a 38 bit integer: 249976000567

```
N = 249976000567
primes = calculate_primes_up_to(N)
s, t = naive_factor(N, primes)
print(s, t, s * t)
```

Never completed on my machine. A 25 bit key solved in over 5 hours.

RSA challenges solved up to 829 bits

Guess and check



N=15

1. Guess g = 3
2. gcd(15, 3) == 3
3. Found factors: 3, 5

N=15

1. Guess g = 7
2. No common divisor
3. Let's improve our guess with $g^{\frac{p}{2}} - 1$
4. Trying p=2
5. New guess $7^{\frac{2}{2}} - 1 = 7 - 1 = 6$
6. gcd(15, 6) == 3
7. Found factors: 3, 5

N=15

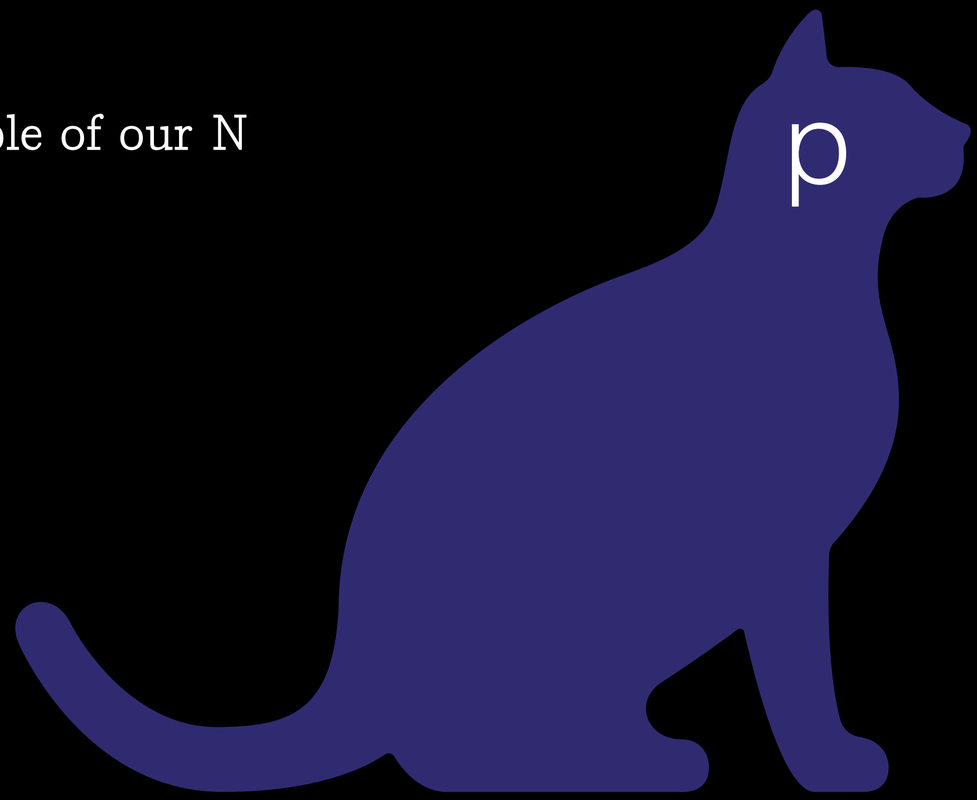
1. Guess g = 2
2. No common divisor
3. Let's improve our guess with $g^{\frac{p}{2}} - 1$
4. Trying p=2
5. new guess: $2^{\frac{2}{2}} - 1 = 2 - 1 = 1$
6. 1 is a trivial divisor and is rejected
7. Let's use $g^{\frac{p}{2}} + 1$ instead
8. new guess: $2^{\frac{2}{2}} + 1 = 2 + 1 = 3$
9. gcd(15, 3) == 3
10. Found factors: 5, 3

But sometimes we don't get an answer

1. Guess g = 14
2. gcd(15, 14) == 1 is trivial
3. Trying to find p for g=14
4. Trying p=2
5. fail
6. Trying p=4
7. fail
8. Trying p=6
9. fail
10. Trying p=8
11. fail
12. Trying p=10
13. fail
14. ...

p is the problem

- For large values of N, it becomes hard to find the right p
- Reflecting on this method
  - We have $(g^{\frac{p}{2}} + 1) \times (g^{\frac{p}{2}} - 1) = m \times N$
  - Multiplying our two guess candidates we get some multiple of our N
- Multiply this out
  - $g^p = m \times N + 1$
  - Special case of $g^p = m \times N + r$
  - Meaning g^p is some multiple of N plus a remainder



$N = 15, g = 7$

$$g^x = m \times N + r$$

$$7^0 = 1 = 0 \times 15 + 1$$
$$7^1 = 7 = 0 \times 15 + 7$$
$$7^2 = 49 = 3 \times 15 + 4$$
$$7^3 = 343 = 22 \times 15 + 13$$
$$7^4 = 2401 = 160 \times 15 + 1$$
$$7^5 = 16807 = 1120 \times 15 + 7$$
$$7^6 = 117649 = 7843 \times 15 + 4$$
$$7^7 = 823543 = 54902 \times 15 + 13$$
$$7^8 = 5764801 = 384320 \times 15 + 1$$
$$7^9 = 40353607 = 2690240 \times 15 + 7$$

N = 15, g = 7

$$g^x = m \times N + r$$

$7^0 = 1 = 0 \times 15 + 1$
$7^1 = 7 = 0 \times 15 + 7$
$7^2 = 49 = 3 \times 15 + 4$
$7^3 = 343 = 22 \times 15 + 13$
$7^4 = 2401 = 160 \times 15 + 1$
$7^5 = 16807 = 1120 \times 15 + 7$
$7^6 = 117649 = 7843 \times 15 + 4$
$7^7 = 823543 = 54902 \times 15 + 13$
$7^8 = 5764801 = 384320 \times 15 + 1$
$7^9 = 40353607 = 2690240 \times 15 + 7$

We need to find p so that

$$g^{1+0} \cong g^{p+x} \cong g^{2p+x} \cong \cdots \pmod{N}$$

$N = 15, g = 7$

$$7^0 = 1 = 0 \times 15 + 1$$
$$7^1 = 7 = 0 \times 15 + 7$$
$$7^2 = 49 = 3 \times 15 + 4$$
$$7^3 = 343 = 22 \times 15 + 13$$
$$7^4 = 2401 = 160 \times 15 + 1$$
$$7^5 = 16807 = 1120 \times 15 + 7$$
$$7^6 = 117649 = 7843 \times 15 + 4$$
$$7^7 = 823543 = 54902 \times 15 + 13$$
$$7^8 = 5764801 = 384320 \times 15 + 1$$
$$7^9 = 40353607 = 2690240 \times 15 + 7$$

There is a pattern to the remainders

$N = 15, g = 7$

$7^0 = 1 = 0 \times 15 + 1$

$7^1 = 7 = 0 \times 15 + 7$

$7^2 = 49 = 3 \times 15 + 4$

$7^3 = 343 = 22 \times 15 + 13$

$7^4 = 2401 = 160 \times 15 + 1$

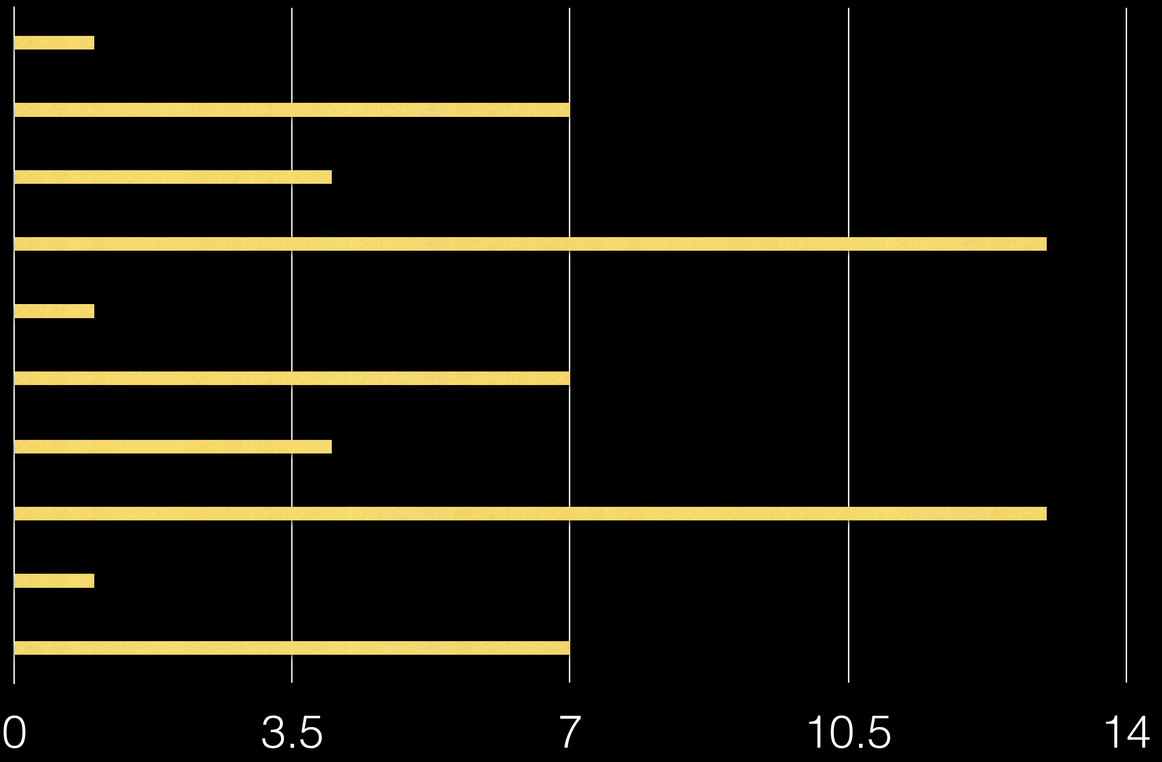
$7^5 = 16807 = 1120 \times 15 + 7$

$7^6 = 117649 = 7843 \times 15 + 4$

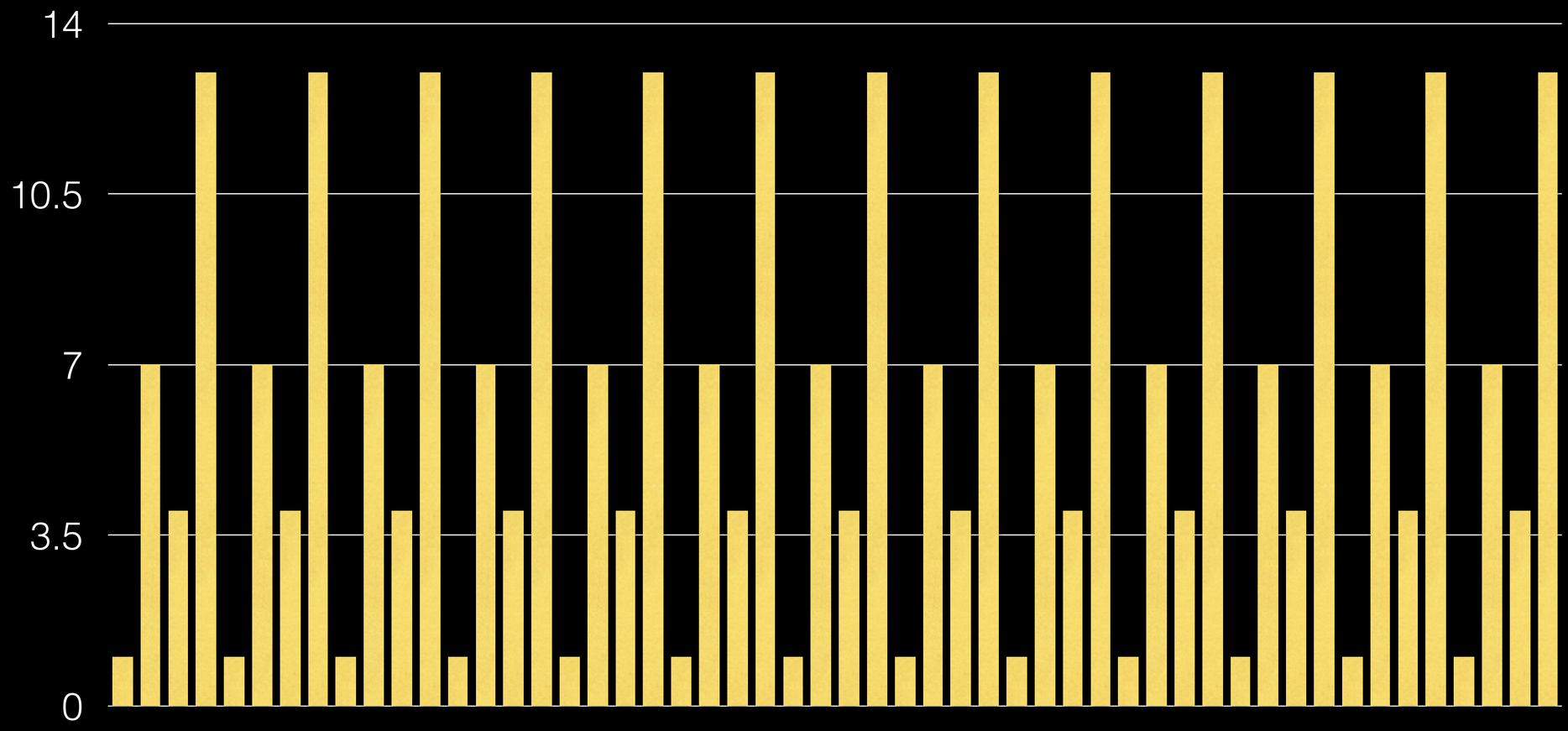
$7^7 = 823543 = 54902 \times 15 + 13$

$7^8 = 5764801 = 384320 \times 15 + 1$

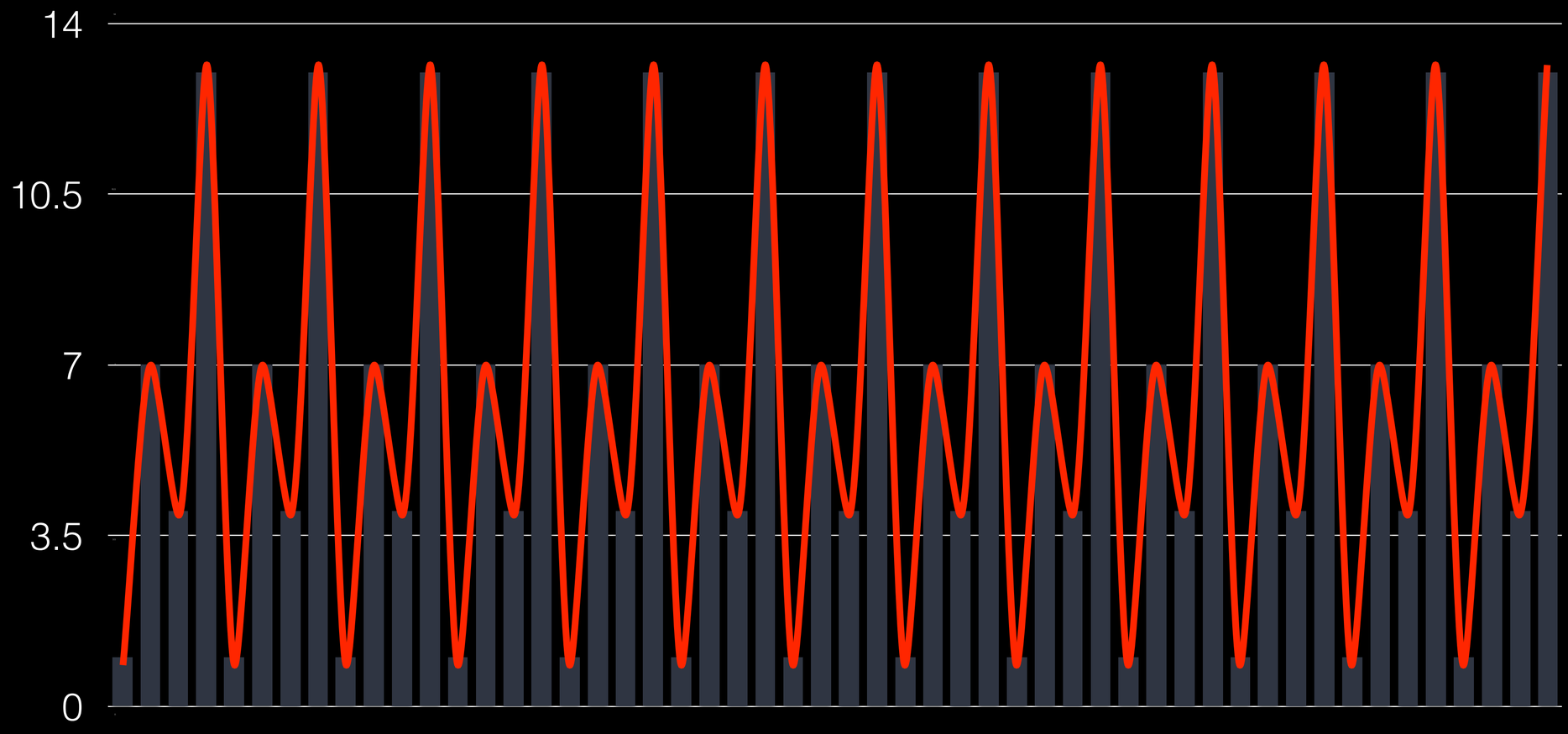
$7^9 = 40353607 = 2690240 \times 15 + 7$



$N = 15, g = 7$

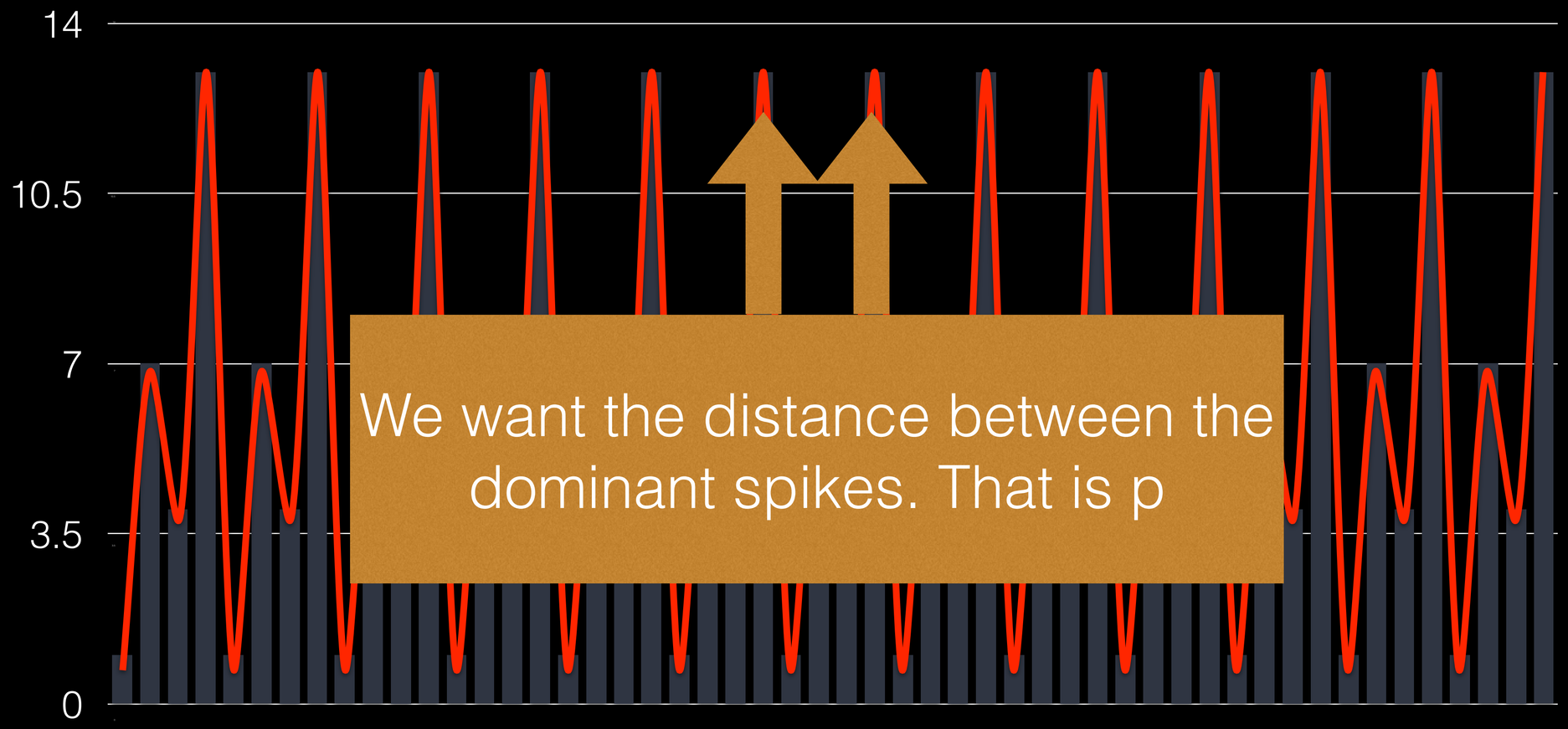


$N = 15, g = 7$



The remainders look like a signal

$N = 15, g = 7$

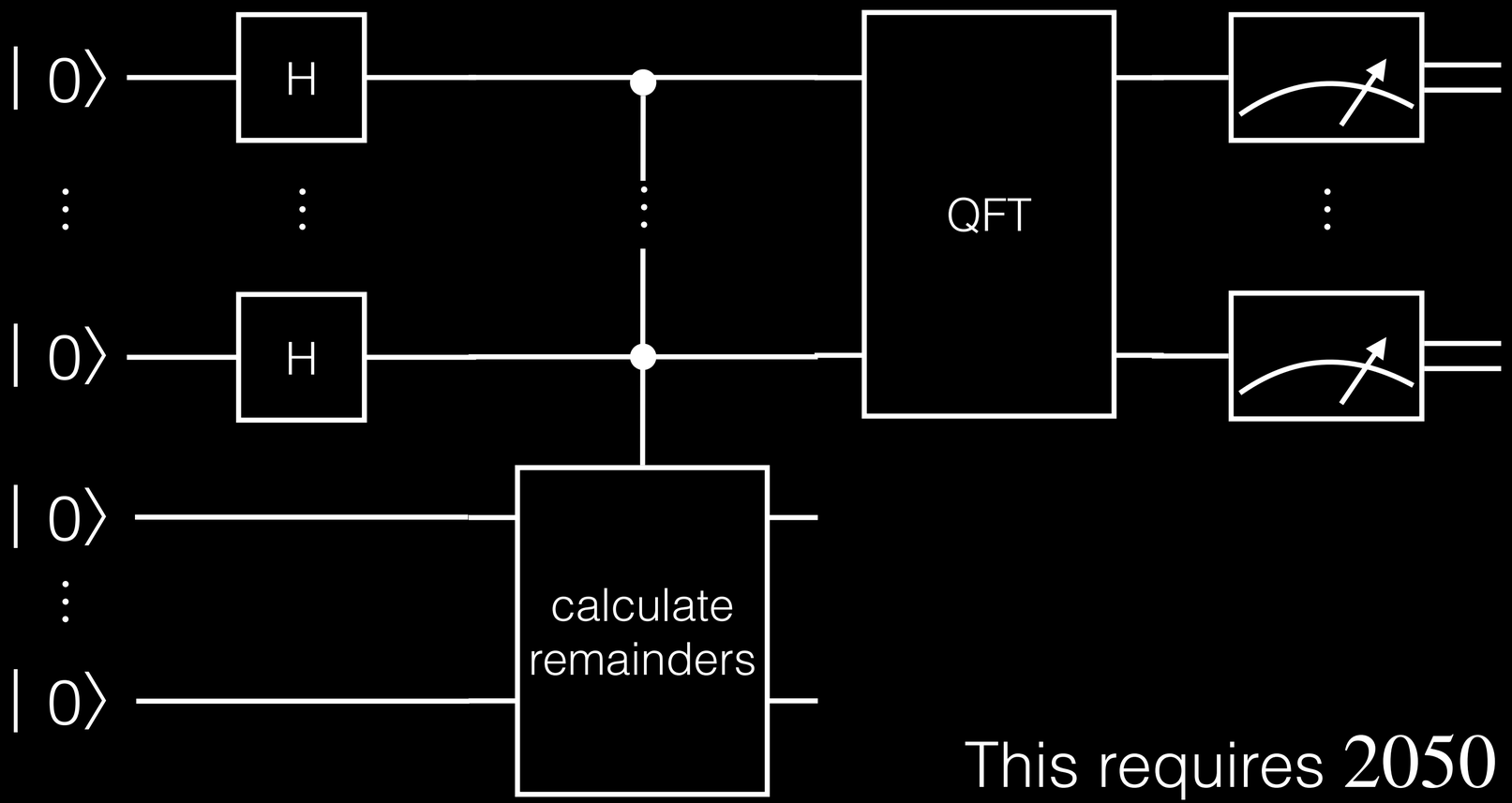


Can we use a Fourier Transform?

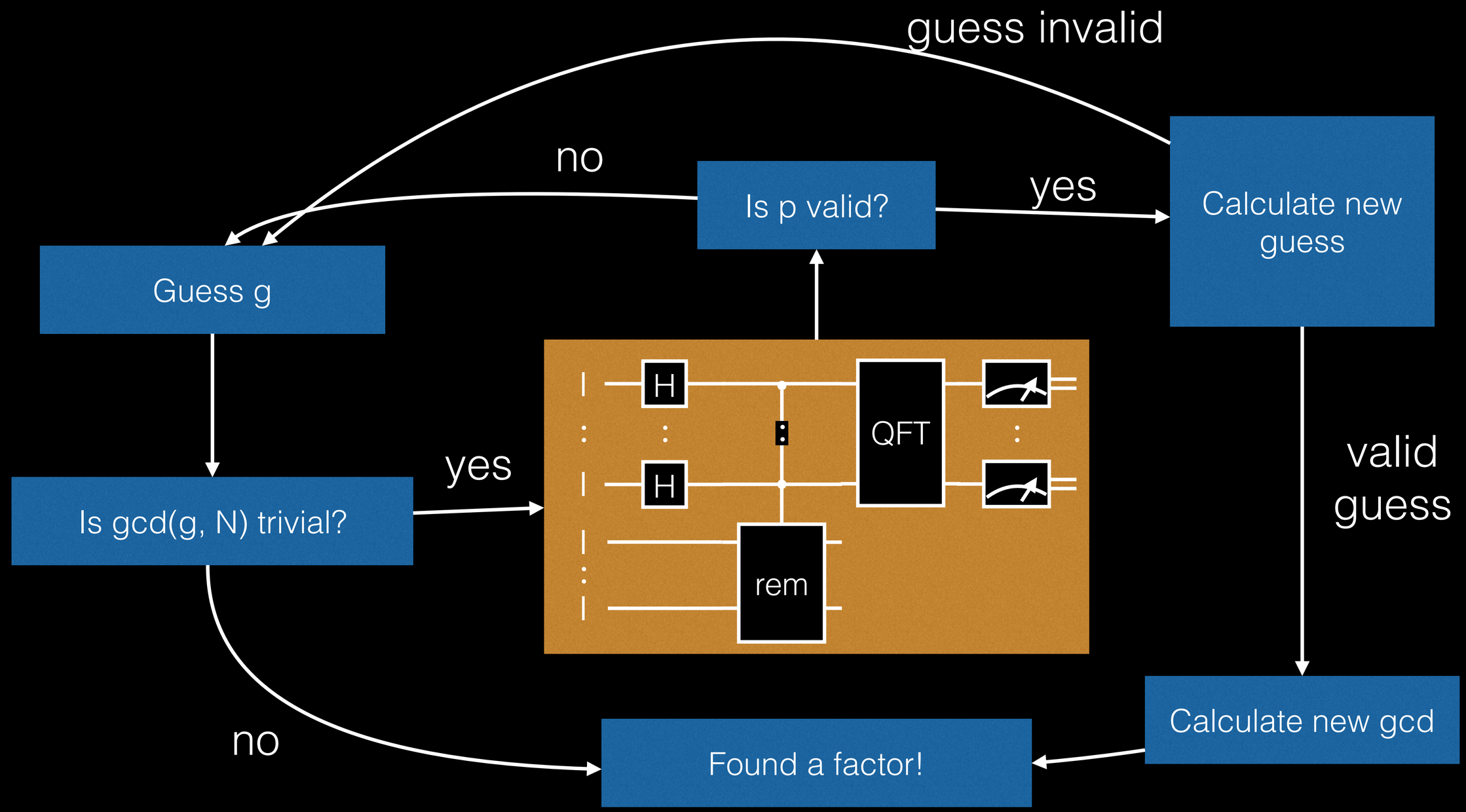
The trouble starts

- Fourier Transforms can help us find the composite wave functions
- And therefore the dominant wave
- BUT, 'Fast' Fourier Transforms are not fast enough for large N
- Enter the Quantum Fourier Transform

By Lucas V. Barbosa - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=24830373

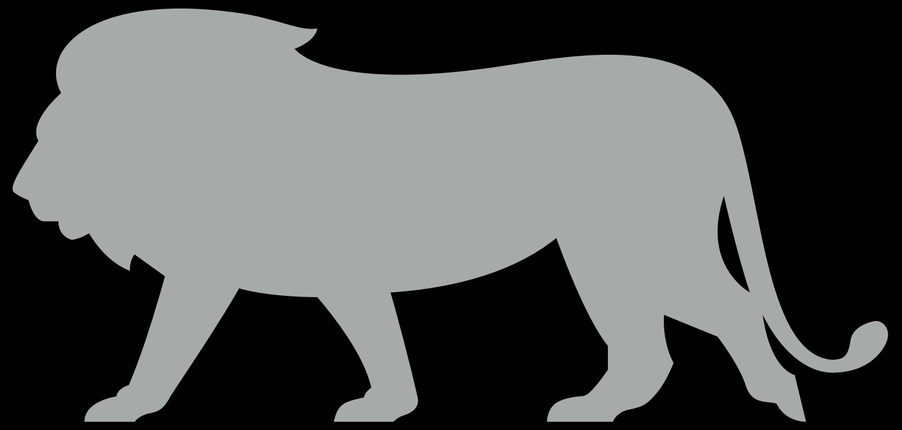


This requires 2050 completely noise-free qubits and $4.81 \cdot 10^{12}$ gates for RSA-1024


guess invalid
no
Is p valid?
yes
Calculate new guess
Guess g
H
H
QFT
rem
yes
Is gcd(g, N) trivial?
valid guess
no
Calculate new gcd
Found a factor!

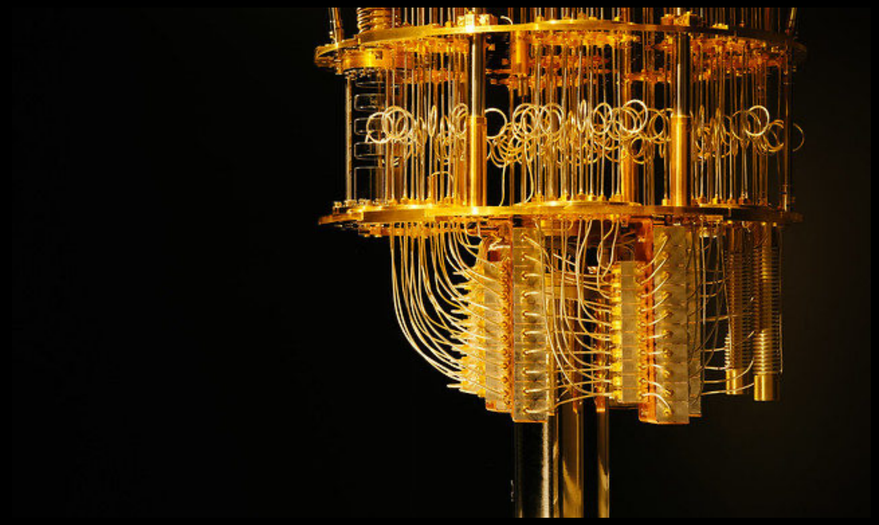
Conclusions

- We can break RSA
- This allows for the Harvesting Attack
- Discrete logarithmic problems 'reducible' to integer factorization
  - so, DHE and ECDHE will also be broken
- But it needs a sh*t-ton of qubits and gates



Interlude: Symmetric cryptography and hashing

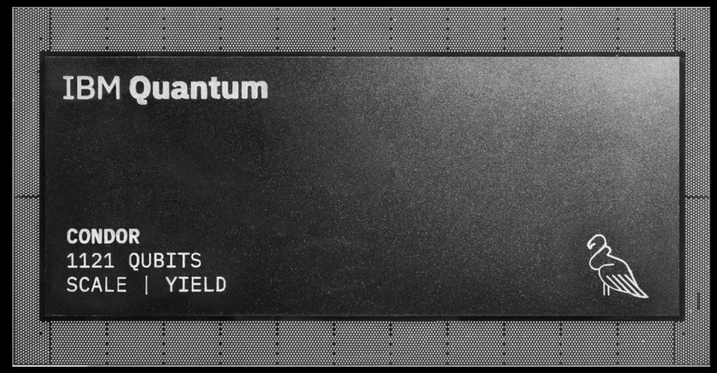
- AES
  - Normally, search space of AES-128 is 2^{127}
  - Grover's speeds this up to 2^{64}
  - Therefore, why worry? Use AES-256 and be happy! For now
- Hashing
  - Also attackable by Grover's
  - But doubling the hash size will protect you for a generation



How real is the threat?

Quantum Computers are not there yet

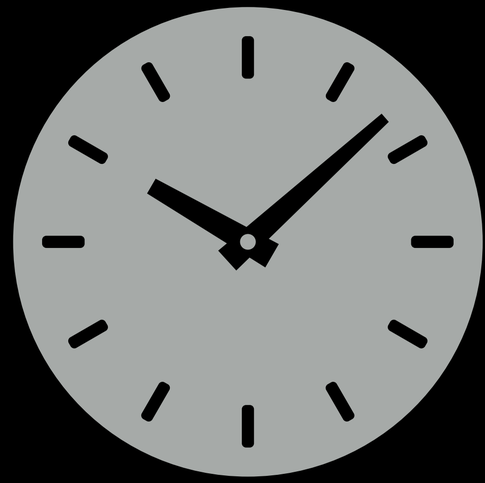
- Three criteria: Qubit count, gate count, gate performance
- IBM's Condor QPU is 1121 qubits with the maybe >1000 gates
  - IBM Heron has better gate performance but only 133 qubits
- These are noisy qubits
  - Noise mitigation requires 10-100x number of qubits!
- Horizontal scaleout will need a rethink of algorithms



Remember what we said:

"This requires 2050 *completely noise-free qubits and* $4.81 \cdot 10^{12}$ *gates for RSA-1024"*

The 'if's

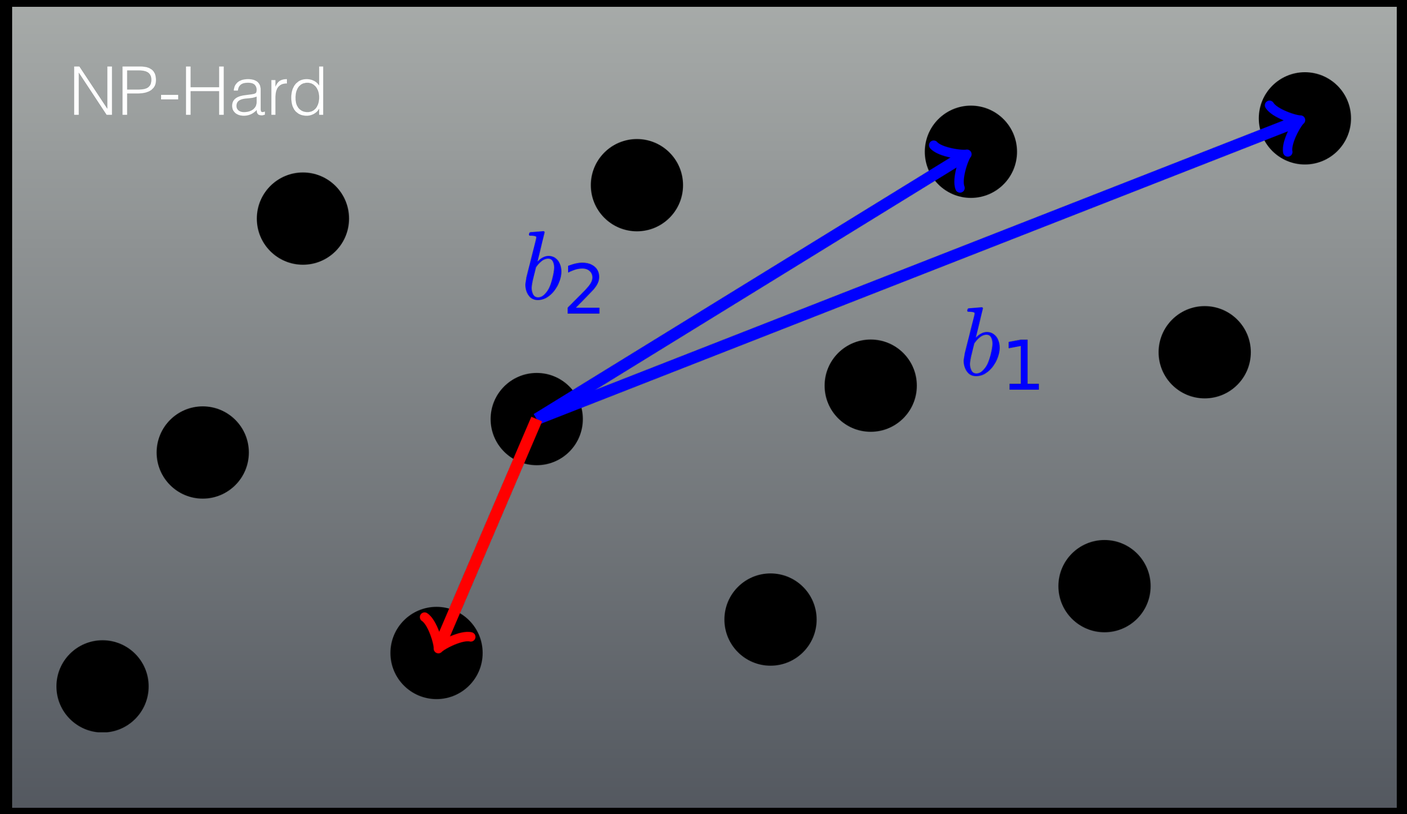


- 5 years from usable machines
- 10 years away from breaking Shor's
- But this could be brought forward if
  - There is a major breakthrough in noise reduction
  - Horizontal scaling does not impact performance
  - A new approach to factoring is found

What can we do about it?
Post-Quantum Cryptography

The approaches

- Learning with Errors
- Lattice-based
- Isogenies
- Code-based
- Hash-based



The shortest vector problem

Key Establishment Candidates

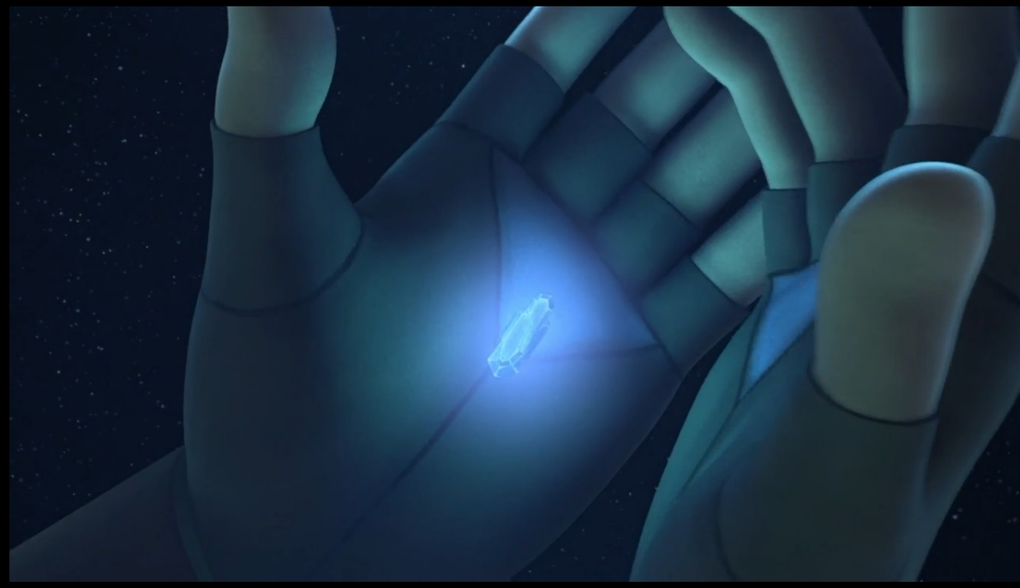
Algorithm	Standard	Assumption	Status
ML-KEM ~~CRYSTALS-KYBER~~	FIPS 203	Lattices&LWE	Will be standardized
Classic McEliece		Code	Round 4
BIKE		Code	Round 4
HQC		Code	Round 4
~~SIKE~~		~~Isogenies~~	Retracted

Digital Signature Candidates

Algorithm	Standard	Assumption	Status
ML-DSA ~~CRYSTALS-DILITHIUM~~	FIPS 204	Lattice	Will be standardized
FALCON		Lattice	Will be standardized (probably as FN-DSA and FIPS-206)
SLH-DSA ~~SPHINCS+~~	FIPS 205	Hash-based	Will be standardized
XMSS	RFC 8391		
Leighton-Micali	RFC 8554		

ML-KEM

- Was CRYSTALS-KYBER
- First implementation bugs found
- So far, no protocol weaknesses
- Approximate 3× slower than ECDH
- Nearly 25× the key size



ML-DSA

- Was CRYSTALS-Dilithium
- Approximately 5× slower than ECDSA for signing.
- Verification is fast though
- About 41× larger public keys

SLH-DSA

- Was SPHINCS+
- Also very slow signing
- But fast verification
- Signatures can be 40k in size

Falcon (FN-DSA?)

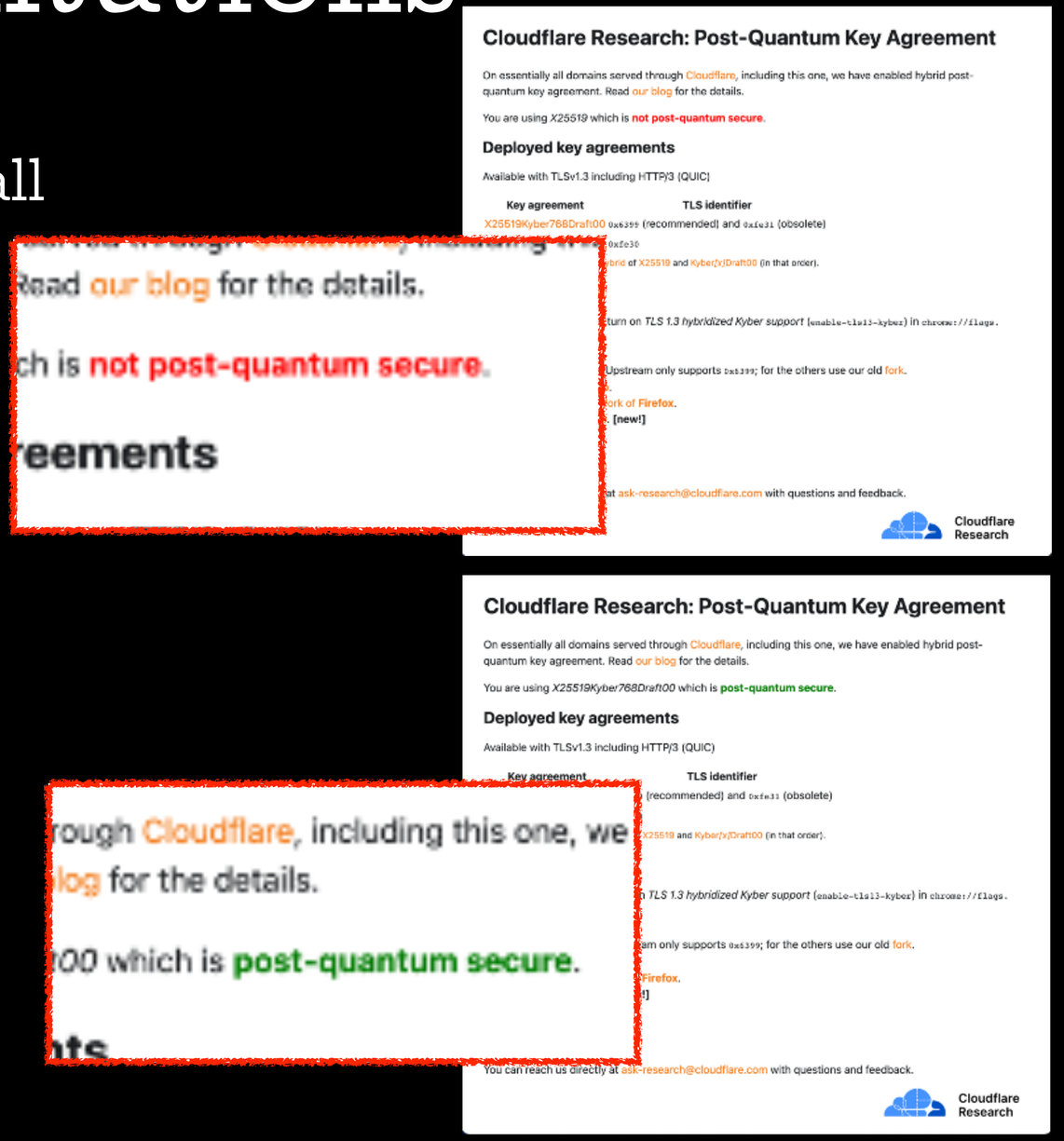
- Was and still is Falcon
- FFT over NTRU-Lattice
- Uniquely, it relies on floating point operations
- Hard to implement
- Not yet standardized but expected this year

Others

- SIKE vulnerability demonstrates risk
  - Follow German BSI advise: go hybrid
- What's up with FrodoKEM and NTRU Prime?
  - BSI still recommends FrodoKEM-976, FrodoKEM-1344 and Classic McEliece

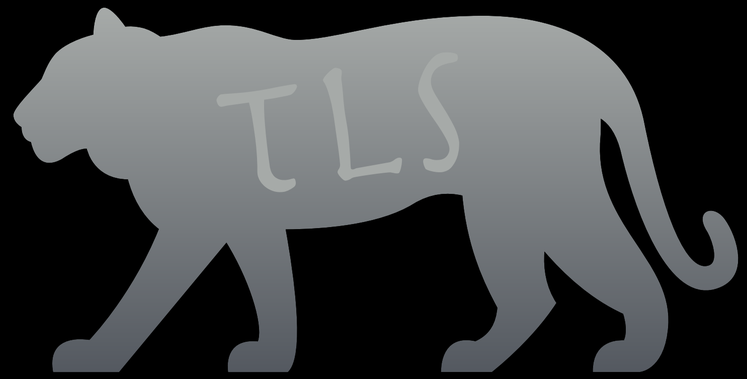
Implementations

- Open Quantum Safe liboqc supports all candidates ++ ->
  - OpenSSL somewhen?
  - OpenSSH > 9.0
  - Wireguard (using Rosenpass)
- AWS, Cloudflare,..
- Chrome, Signal, iMessage, ...



TLS 1.3

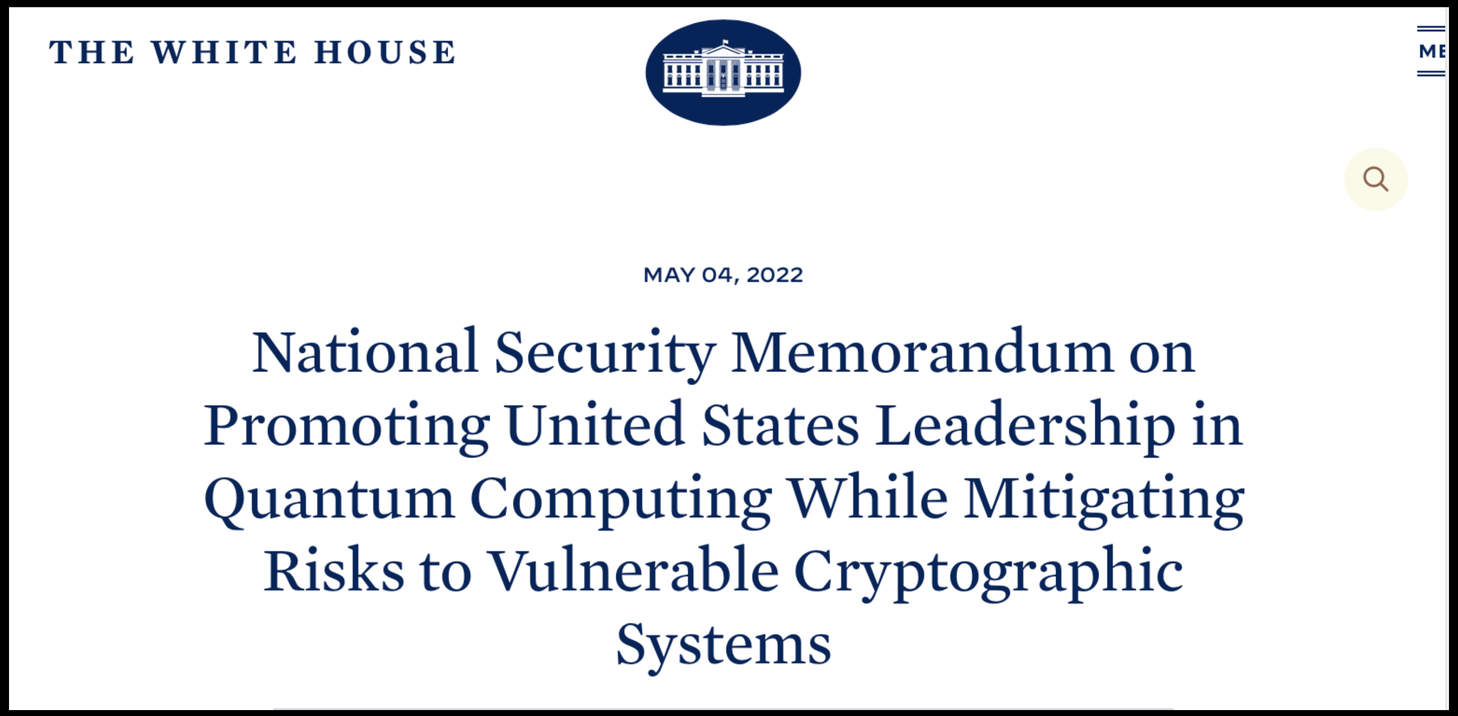
- In draft mode:
  - ML-KEM-512, ML-KEM-768, and ML-KEM-1024
  - Hybrid approach being discussed
- Cloudflare:
  - Two percent of all TLS 1.3 are ML-KEM
- Implementations
  - BoringSSL, WolfSSL
- But no OpenSSL suport yet



OpenSSH

- From 9.9 onwards
- Hybrid approach
  - ML-KEM and ECDH

PQC by 2035 (USA)



"the goal of mitigating as much of the quantum risk as is feasible by 2035"

Name confusion

- ML-KEM = FIPS 203 = CRYSTALS-Kyber = PQ3 (Apple)
- ML-DSA = FIPS 204 = CRYSTALS-Dilithium
- SLH-DSA = FIPS 205 = SPHINCS+
- (FN-DSA = FIPS 206 = Falcon ???)

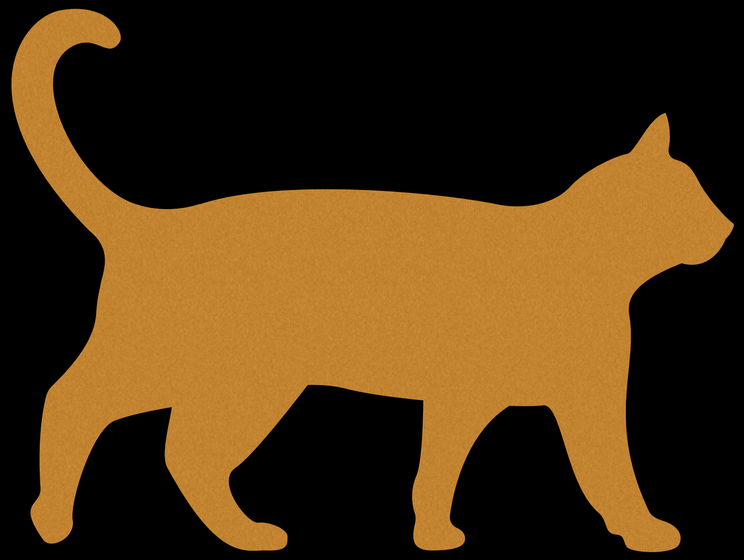
????

Quantum Key Distribution/BB84

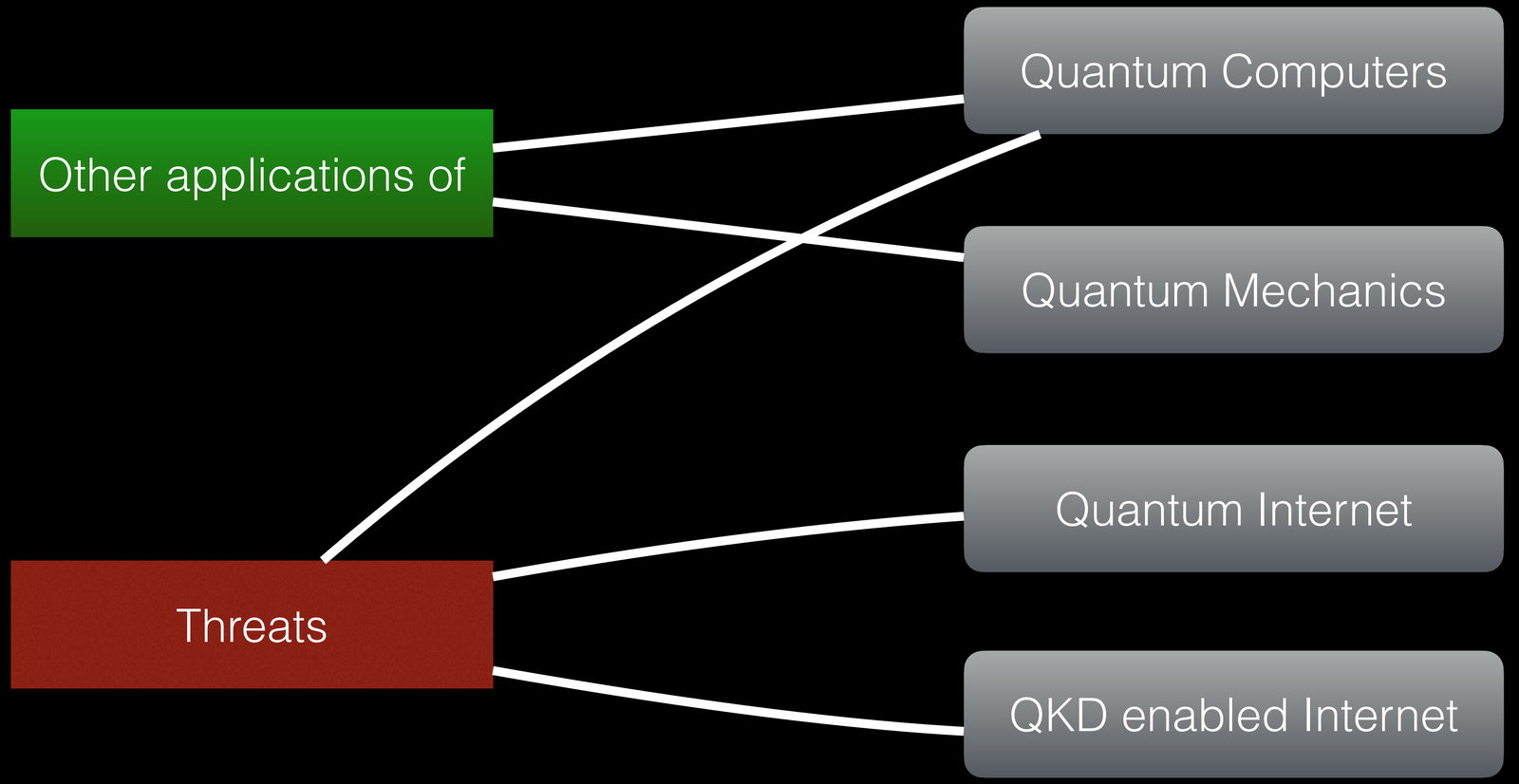
- Provably secure
  - less sure about practical implementations
  - Limited usability
- Quantum Digital Signatures schemes also becoming usable

Main takeaway IMHO

- Threat to asymmetric cryptography is theoretically real
- > 10 years until sufficiently large quantum computers exist
- But the harvesting attack needs to be considered!
- Start planning now
  - PQC needs more space and time
  - Challenging in OT environments
- Otherwise, wait until vendors do the work for you



What I'm watching



Will AI/ML eat quantum computer's lunch?

https://www.trendmicro.com/vinfo/us/security/news/security-technology/...
diving-deep-into-quantum-computing-modern-cryptography
diving-deep-into-quantum-computing-computing-with-quantum-mechanics
post-quantum-cryptography-quantum-computing-attacks-on-classical-cryptography
post-quantum-cryptography-migrating-to-quantum-resistant-cryptography
the-realities-of-quantum-machine-learning